February 2011

MONTHLY Cyber Security Newsletter

Security Tips

Mississippi Department of Information Technology Services

Division of Information Security

This issue…

This month's newsletter discusses Cyber Ethics and the potential threats that lie dormant in USB devices.

Who Should Be Concerned About Cyber Ethics

Cyber ethics must be taught and reinforced at every level of computer use—from the novice user just learning to navigate a computer and the Internet, to an information professional whose job requires significant use of online resources. In the same way that each culture teaches its citizens the ethics of business, education, government, etc., those who use the Internet must be taught ethical practices in every aspect of its use.

Why Should We Be Concerned About Cyber Ethics?

The power of the Internet means that anyone can communicate at anytime, with anyone, anywhere. While this has undeniable benefits, there can also be negative consequences. Anonymous posting to blogs, websites and social media can encourage bad behavior by eliminating the need to stand behind the words used. A significant issue of increasing concern is cyber bullying. What were once comments confined to the school yard or hallways are now magnified by the power and anonymity of the Internet. Developments in electronic media offer new forums for bullies, and the actions can range in severity from cruel or embarrassing rumors to threats, harassment, or stalking. The effects can be far-reaching and long lasting.

What are The Rules Of Ethical Cyber Activity?

The basic rule is do not do something in cyber space that you would consider wrong or illegal in everyday life.

When determining responsible behaviors, consider the following:

- Do not use rude or offensive language
- Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Do not copy information from the Internet and claim it as yours

- Adhere to copyright restrictions when downloading materials, including software, games, movies, or music from the Internet.
- Do not break into someone else's computer
- Do not use someone else's password.
- Do not attempt to infect or in any way try to make someone else's computer unusable.

We were taught the rules of "right and wrong" growing up. We just need to apply the same rules to cyber space!

Resources For More Information:

- Computer Crime & Intellectual Property Section – United States Department of Justice
  - http://www.justice.gov/criminal/cybercrime/cyberethics.htm
- Microsoft Safety & Security Center
  - http://www.microsoft.com/security/online-privacy/cyberethics-practice.aspx
- Cyberbullying Prevention Lessons-NCSA and CyberSmart!
  - http://cybersmartcurriculum.org/cyberbullying/ncsa/
- Teaching your children acceptable behavior on the Internet
  - http://us.norton.com/library/familyresource/article.jsp?aid=pr_cyberethics
- Cyber Citizen Partnership
  - http://www.cybercitizenship.org/

USB Devices: Just How Secure Are They?

AliceClaire Thompson

USB devices are everywhere. From smartphones to portable gaming units, you can find just about anything these days to connect into your USB port. According to Gartner IT research and advisory company, there were roughly 222 million USB devices shipped in 2009. While these devices have become wildly integrated into our daily lifestyle, a growing threat is potentially housed inside: malware. The many conveniences of these devices are becoming overshadowed by the increasing threat of an infected device being connected to your PC. Avast Software reported that in the 700,000 attacks monitored by the firm in the last week of October 2010, 13.5% were the product of infected USB devices. While most users have been educated to understand not to click on links inside emails from unknown senders or offer any confidential information on an unknown or untrusted website, most general users are not aware of the significant threat that lies dormant in a USB device. A study done by PandaLabs discovered around 25% of new worms in 2010 were designed specifically to spread through devices that connect to your PC via a USB port.

The main way malware is delivered by these devices is through the autorun feature in Windows. Autorun is a feature that pops up a dialogue box on your screen when the device is attached to your PC. When the infected USB flash drive or other USB device is connected an executable file starts and begins to download the malware to your computer. While the autorun feature is a convenience that allows users to browse their external devices upon activation, the safest way to protect against this threat is to disable the function.

Interesting Statistics…

A recent study conducted by the data protection company, CREDANT Technologies, reveals that nearly 10% of people who own a USB device containing corporate data have lost it. Even more alarming, 75% of these employees never reported it to their boss.

As threats advance with ever progressing technology, no one solution can keep any network entirely defended from malicious attacks. In the fall of 2008 the U.S. Military had a breach as a result of an infected USB device and the autorun feature. William Lynn, the US Deputy Secretary of Defense, reported in February 2010 that the US military had had an intrusion via a USB thumb drive that occurred in the fall of 2008. Because of this the Pentagon made decision to ban USB thumb drives from the entire military. This was in place until February of 2010. Lynn says that the widespread worm infection entered their system via a US military laptop at a base in the Middle East and was instigated by a foreign intelligence agency. He says, “To stay ahead of its pursuers, the United States must constantly adjust and improve its defenses.” This attack significantly compromised the Pentagon computers in 2008. This was the most significant breach of US military computers ever and served as an important wake up call, Lynn said.

Even well established and notable technology companies, such as IBM, have fought this battle. At an Australian Computer Emergency Response Team (AusCERT) 2010 conference in Queensland, Australia, IBM gave away USB drives that were unknowingly infected with malware. All attendees were instructed by IBM’s headquarters not to use to device and to return it back to IBM.

As is with any threat, staying up to date on education about new and coming threats is the best way to initiate your most effective defense. Disable the autorun feature on your machine and make sure that you always have the most current version of your anti-virus software. Above all else, never allow any USB device to run on your machine prior to scanning it. Putting all of these tips into practice will give you the very best chance of keeping the malicious attacks at bay.

this newsletter is brought to you by…

MS-ISAC

www.msisac.org

ITS

www.its.ms.gov/services_security.shtml